NETCOM / 9th Army Signal Command

Legal Issues and Information Systems Operations

TOM KING
SJA ATTORNEY-ADVISOR
(520)533-3197 DSN 821-3197
TOM.KING @NETCOM.ARMY.MIL

This briefing will discuss legal issues.

For legal answers, consult your
own attorneys.

OVERVIEW

Constitutional Basis

Congressional Approach - statutes

Regulations

BACKGROUND FOR LEGAL ISSUES

-- U.S. Constitution:

-- 4th Amendment (protection from unreasonable search and seizure)

-- Equal Protection

-- 1st Amendment (Free Speech)

United States v. American Library Assn. 02-361 June 23, 2003

-Law requiring public libraries and schools that receive federal funds to install internet blocking software – Supreme Court overrules E.D. P.A. Supreme Court holds that libraries' use of Internet filtering devices does not violate patron's 1st amendment rights.

First Amendment - Free Speech Issues

Urofsky v. Gilmore 167 F.3d 191 (4th Cir. 1999), Certiorari Denied 121 S.Ct. 759 (January 8, 2001) - Virginia Law prohibiting Commonwealth employees from using Commonwealth computers for "sexually explicit content" upheld -- cites:

Connick v. Myers 461 US 138 (1983) Distinguishes 1st Amendment rights of citizens from rights of public employees speaking as public employees - If a public employee's speech does not touch upon a matter of public concern, it is subject to regulation without violating 1st Amendment

First Amendment - Free Speech - Equal Protection Issues

WE CAN LEGALLY BLOCK OUTGOING TRAFFIC FROM GOVERNMENT EMPLOYEES, BUT….

What about the rights of those we block?

CAN WE BLOCK INCOMING:

- Attacks?
- Commercial Solicitation?

Fourth Amendment - Privacy Issues

O'Connor v. Ortega 409 US 709, 107 S. CT 1492 (1987)

-Confirms 4th Amendment protection in the government workplace.

-Establishes a Reasonableness Test on a case by case basis.

-Distinguishes administrative employer search from law enforcement search.

Fourth Amendment - Privacy Issues

US v. Simons 29 F. Supp. 2d 324 (EDVA, 1998)

CIA employee had no expectation of privacy on his CIA computer because of a policy that said that computer use would be audited, to include web sites visited, URL pages retrieved, inbound and outbound file transfers, sent and received e-mails.

AFFIRMED IN PART -REMANDED IN PART ON OTHER GROUNDS 206 F.3rd 392 (2000) Motion denied on remand by ED

U.S. V. MONROE (50 MJ 550) affirmed 52 MJ 326 (2000)

Air Force Regulation that advised personnel their e-mails were subject to monitoring defeated expectation of privacy so that System Administrator could read e-mails without a warrant.

UNITED STATES v. GETER
NMCM 9901433, May 20, 2003

- Marine uses government e-mail for marijuana distribution scheme. SA informs JAG that Geter's email contents are on government system and contents were "large". SA allows JAG access. Court holds no expectation of privacy, no 4th amendment violation.

- Also holds evidence would have been "inevitably discovered" anyway.

U.S. v. SIMS (DC New Mexico 2001)

System Administrator acted as a tool of law enforcement when he searched Sims files on employers' systems at the request of FBI - evidence is subject to exclusion

Banner Warning Doesn't Waive 4th Amendment Protection

No Privacy Expectation Against

Wiretap Statutes and Electronic Communications Privacy Act

18 USC 2510-2521 and 2701

- The Wiretap (Title III) Statute
- Prohibits Unauthorized Interception, Use, or Disclosure of Wire, Wireless, Oral or Electronic Communications
- Stored Wire Communications
- Limited Exceptions are Found in the Statute

5 ECPA EXCEPTIONS:

1. Business Extension (doesn't apply to e-mail)
2. Pursuant to Legal Process (Warrant)
3. COMSEC activities conducted in accordance with Attorney General Approved Procedures (AR 380-53)
4. Service Provider Exception . . . May intercept, use or disclose communications while engaged in any activity which is necessarily incident to the rendition of the service or the protection of the rights or property of the service provider (AR 25-2)
5. Consent to Monitor - ONE PARTY CONSENT. May Be Express or Implied, But Implied is Weaker - Look at ALL the Circumstances

CONSENT TO MONITOR

O'Connor v. Ortega 480 US 709 (1987)

Banner Warning didn't waive 4th amendment (SIMS)

Expressed Consent

- Explicit Verbal or Written Permission
- Signed User Agreements
- Consent form
- Banner Warnings with Affirmative Action Requirement

Implied Consent

- Warning Banners
- Policy Letters
- Orientation Briefings
- Notices in Bulletins or Newspapers

DISCLOSING INTERCEPTED COMMUNICATIONS

<u>Limited Disclosure Under ECPA</u>

- Other Service Providers and Employees
- Parties
- Pursuant to Authority of Statute, Court Order or Foreign Intelligence Surveillance Act
- To Law Enforcement If Information Appears to Pertain To Commission of Crime and Was Inadvertently Obtained

Foreign Intelligence Surveillance Act
50 USC § 1809

Prohibits government employees from engaging in electronic surveillance except as authorized by statute

Prohibits disclosing information obtained under color of law by electronic surveillance if not authorized by statute.

COMPUTER FRAUD AND ABUSE ACT
"HACKER STATUTE"
18 USC § 1030

Also known as The "Hacker Statute"

Prohibits Accessing Computer Without Authority or Exceeding Authority

Prohibits implanting malicious code or virus

Sliding Scale of Punishment Based on Intent and Damage Caused

Exception for Law Enforcement or Intelligence Agency

REGULATIONS

1. AR 25-2 sets guidelines and limits for System and Network Administrators

2. AR 380-53 - "Information Systems Security Monitoring" - Rules and Limitations on Security Monitoring

3. Joint Ethics Regulation - Rules for Users

DoD 5500.7R

AR 25-2, Chapter 4

The Network or System Administrator may monitor their own systems to ensure proper performance and management.

Limitation is that of service provide exception, necessary to keep service operational or protect rights and property of the service provider. (Obtain guidance from legal counsel)

Can only use CIO/G6 approved NETCOM configured tools

Cannot target individuals for monitoring

Can assist proper Law Enforcement/Counterintelligence investigations

AR 25-2

SA/NA cannot browse or read user's e-mail without incident specific consent or as part of properly authorized investigation.

SA/NA cannot let a supervisor into user's data files.

SA/NA can assist a management search only when employee is absent to find file for official purpose. Employee must then be notified and MFR created.

AR 380-53

Only authorized individuals as set forth in the regulation can conduct information systems security monitoring.

Cannot monitor for intelligence, law enforcement, or disciplinary reasons – exception for C2 protect functions.

Limited to vulnerability assessments for systems under the direct control of System and Network Administrators.

Joint Ethics Regulation DoD 5500.7R, Para. 2-301

Contains the Rules For DoD Personnel's Use of Government Telecommunications resources.

Limited Personal Use of Government Internet.

- Off Duty
- No Pornographic or Gambling Sites
- No streaming data flow

Limited Personal Use of Government E-mail.

- No Chain Letters
- No Commercial Business

If Policy in Place and Doesn't Overburden the System.

JER 2-301 a. (3)

DoD employees shall use federal government communications systems with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized

CARLOS MORRISON v. NASA 65 M.S.P.R. 348 (1994), 35 day suspension for having sexually explicit pictures on government computer, and exposing co-workers to sexually explicit material held not excessive.

CLINTON ZIMMERMAN v. PIRIE SEC NAV, 101 FEOR 1223 (April 5, 2001) 3 day suspension for viewing pornography

WHY WORRY?

Subject to Civil and Criminal Suit if You Exceed your Authority

Under ALL THREE STATUTES you can be sued by Party to the communication or someone Against whom the interception was directed

ONE ARMY SA PROSECUTED

CYBER SPACE RULES OF THE ROAD

- Strict compliance with Law & Regulation
- Clearly Identify the Purpose of Monitoring
- Following correct procedure is always the safest approach
- Get permission of System Owner in Writing
- Use Procedures and Software that will give you a good audit trail
- Know when to call in Law Enforcement and Counter Intelligence